IN FOCUS: FREQUENTLY ASKED QUESTIONS ABOUT

What is personal operational security?

Operational security is guarding information to help ensure that military operations stay safe, secure, and secret from enemy forces. This can include information such as troop numbers, times, dates, locations, troop strength, equipment availability, operation names and other data.

Personal OPSEC is what *you* as an individual can do to help maintain operational security.

Why is personal operational security important?

Because the enemies we fight are constantly looking to gather as much information as they can about our military operations and capabilities, safeguarding that information is the responsibility of everyone in the military community who may have access to it.

What is the real threat here?

Terrorist organizations are constantly trying to gather information on U.S. military operations. Some of the information they look for isn't even classified, but it is still hard for someone outside the military community to obtain. Never underestimate the information you have – what you take for granted may be valuable intelligence to the enemy.

What kind of information is the enemy looking for?

(Taken from the Al Qaeda training manual)

- Names / photographs
- Information about tactics, techniques and procedures
- Information about equipment vulnerabilities
- Present and future capabilities
- Insights into national or military morale
- When and where meetings of top military or diplomatic officials will take place
- Information about important government places
- Information about military facilities, including:
    - Location
    - Units
    - Weapons used or available
    - Fortifications and tunnels
    - Amount of lighting
    - Exterior size and shape
    - Number of personnel
    - Ammunition depot locations
    - Leave policies
    - Degree and speed of mobilization

What are some basic guidelines about things I should not talk about?

- Dates and times, such as the starting or ending times of operations and flight information for Soldiers deploying or redeploying.
- Size and strength of forces.
- Any shortfalls in manning or equipment.
- Mission details, such as the start or end times, objectives, call signs, operation name, etc.
- Any flaws in base security, antiterrorism or force protection measures. These should be reported, not talked about.

What should family members know about OPSEC?

OPSEC applies to family members, too. Know that by following good OPSEC practices you're helping to keep your Soldier safe and secure.

The most typical scenario for family members and OPSEC relates to learning about flight dates and times for their Soldiers who are deploying or redeploying. Although it's important to make plans for these events, you should not talk about any specific dates or times with anyone. Ambiguous replies to extended family are usually best. When in doubt, "I'll let you know as soon as he gets back" is safe.

What are the most common mistakes people make with regard to OPSEC?

- Revealing important information online, particularly in forums, chat rooms, on Facebook, or other public and social media or social networking sites.
- Complaining about not having enough equipment or having enough people. This kind of information is exactly what the enemy wants to hear.